シローおよびフロベニウスの定理を結ぶゼータ関数(代数的組合せ論)

AUTHOR(S):

吉田, 知行

CITATION:

吉田, 知行. シローおよびフロベニウスの定理を結ぶゼータ関数(代数的組合せ論). 数理解析研究所講究録 1991, 768: 1-15

ISSUE DATE:

1991-11

URL:

http://hdl.handle.net/2433/82337

数理解析研究所講究録
第768巻 1991年 1-15

シローおよびフロベニウスの定理を結ぶゼータ関数

吉田知行 (Tomoyuki YOSHIDA　北大・理)

概略： 有限群における部分群の個数や、その群上の方程式の解の個数は古くから研究されてきた。ここでは母関数の理論からのアプローチを試みる。応用として、無限乗積に関するオイラーやコーシーなどの恒等式、有限アーベル群に関するホールの奇妙な等式を証明する。

キーワード： シローの定理、フロベニウスの定理、合同式、群の準同型、群上の方程式、オイラー標数、母関数、ゼータ関数、LDU-分解、メビウス関数、有限アーベル群、分割数、コーシーの恒等式、指数公式

1. シローおよびフロベニウス型合同式

G は有限群、p は素数とする。群論の創世期からある古い問題として次のふたつがある。

シロー型の問題： 有限群における、与えられた型の部分群の個数に関する合同式。

フロベニウス型の問題： 有限群上の方程式の解の個数に関する合同式。

これらは、今から50年以上前、盛んに研究されていた。いくつか例をあげておこう。

Sylow (1872): G のシロー p-部分群の個数について、

$$\boxed{|\mathrm{Syl}_p(G)| \equiv 1 \mod \gcd(n, |G|)}$$

シローが1872年という古い時期にこの定理を得ているのは驚きである。シロー (1832-1918) はノルウェーの数学者で、その業績とエピソードについては伊藤昇先生の記事 [It 89] がある。この定理の拡張フロベニウスにより得られている。

Frobenius (1895): p^i が G の位数を割り切るなら、位数 p^i の G の部分群の個数は p を法として1に合同である。

次は、フロベニウス型問題に対する、最初の成果である。

Frobenius (1903): 自然数 n に対し、

$$\boxed{\sharp\{x \in G \mid x^n = 1\} \equiv 0 \mod \gcd(n, |G|)}$$

さらに次のような結果がある。P を G のシロー p-部分群とし、$p^l := |P| = |G|_p$ と置く。

P.Hall(1935): P が巡回群なら、$0 \leq i \leq l$ に対し、

$$\sharp\{H \leq G \mid |H| = p^i\} \equiv 1 \mod p^{l-i+1}.$$

A.Kulakoff (1931) + P.Hall (1935): $p \neq 2$ で P が巡回群でないなら、$0 < i < l$ に対し、

$$\sharp\{H \leq G \,|\, |H| = p^i\} \equiv 1 + p \mod p^2.$$

G.A.Miller (1904): $p \neq 2$ で P が巡回群でないなら、$2 \leq i < l$ に対し、

$$\sharp\{\text{位数 } p^i \text{ の巡回部分群}\} \equiv 0 \mod p.$$

A.Kulakoff (1931): $p \neq 2$ で、G が位数 p^l の非巡回群ならば、$0 < i < l$ に対し、

$$\sharp\{x \in G \,|\, x^{p^i} = 1\} \equiv 0 \mod p^{i+1}$$

ホールの論文 [Ha 35] は、この方面における頂点をきわめたものである。この論文以降研究は下火になる。ホールのこの論文 (結果は複雑で、証明も難解) があったことと、有限群論の研究者の関心が他 (表現論、単純群の分類) に移ったことが理由と思う。

2. ブラウンのホモロジー論的シローの定理

ホールの論文から 40 年たって、ブラウンの定理が現われる。

K.Brown (1975): $\mathcal{S}_p$ を G の nontrivial な p-部分群の成す半順序集合とする。このときそのオイラー標数に関して

$$\boxed{\chi(\mathcal{S}_p) \equiv 1 \mod |G|_p.}$$

$\mathcal{S}_p$ の位相幾何的性質については D.Quillen の論文 [Qu 78] に詳しい。有限順序集合 S の オイラー標数 $\chi(S)$ とは、対応する順序複体 (全順序部分集合の成す単体的複体) のオイラー標数であり、順序集合のメビウス関数を使って表現できる:

$$\chi(S) := \sum_{x,y \in S} \mu(x,y)$$

ここで メビウス関数 $\mu : S \times S \longrightarrow \mathbb{Z}$ は、次の等式を満たすものとして一意的に定義される。

$$\mu(x,x) = 1;\ \mu(x,y) = 0 \quad \text{if } x \not\leq y;$$
$$\sum_{y \leq z} \mu(x,y) = \sum_{y \geq x} \mu(y,z) = \delta_{x,z}, \quad x \leq z.$$

したがって、ブラウンの定理は、部分群束のメビウス関数に関する合同式を与える。

有限群のバーンサイド環の理論 (特にべき等元公式とコーシー・フロベニウスの定理) を使うと、3 種類の合同式 (シロー、フロベニウス、ブラウンのもの) は、容易に証明できる。[Wa 80], [Gl 81], [Yo 83], [DSY ??] 参照。

p-部分群全体でなくても、その部分順序集合のオイラー標数あるいはメビウス関数についても合同式が得られる。例えば [BT 88] がある。ここではバーンサイド環の理論は使われていない。

また [Yo 90] では、部分群の族に関する一般バーンサイド環を導入し、それを用いて合同式を得ている。

3. 新しいフロベニウス型合同式

C_n を位数 n の巡回群、G を有限群とする。このとき (標準的でない) 全単射

$$\mathrm{Hom}(C_n, G) \xrightarrow{\cong} \{x \in G \mid x^n = 1\}$$

がある。対応は、C_n の生成元 a を一つ持ってきて、$\lambda \longmapsto \lambda(a)$ で与えられる。したがってフロベニウスの定理 (1903) は、

$$\boxed{|\mathrm{Hom}(C_n, G)| \equiv 0 \mod \gcd(n, |G|)}$$

と書き換えられる。また群上の方程式の解の個数に関するフロベニウス型の問題も、次のように書き換えられる。

改訂版フロベニウス型問題: ふたつの群 A, G の間の準同型の個数 $|\mathrm{Hom}(A, G)|$ の満たす合同式。

群の準同型の個数を扱った論文はきわめて少ない ([So 69]) 。しかし群上の方程式の解の個数に関する結果はたくさんあり、それらは準同型の個数を用いて書き直せる。例えば、ホールは [Ha 35] の中で、本質的には次の合同式を証明している。

P.Hall (1935): A を (有限または無限) 群、$B \leq A$ 、$x \in A$ で $A = \langle B, x \rangle$ なるものとし、$\mu : B \longrightarrow G$ を有限群 G への準同型とする。このとき

$$\sharp\{\lambda : A \longrightarrow G \mid \lambda_{|B} = \mu\} \equiv 0 \mod \gcd(|C_G(\mu(B))|, |A/[A, A]B|).$$

ここで $[A, A]$ は交換子群、C_G は中心化群を表わす。

P.Hall (1935): P を G のシロー p-群、C_{p^r} を基本可換 p-群とする。このとき、$r \geq 1$ に対し、

$$|\mathrm{Hom}(C_{p^r}, G)| \equiv 0 \mod p^m$$

ここで

$$p^m := \begin{cases} (P : \Omega_1(P)) & P \text{ が正則 } p\text{-群のとき} \\ p^{p-1} & \text{その他} \end{cases}$$

(正則 p-群の定義は [Hu 67] 参照。)

そのほかにも次のような合同式もある ([Yo ??]) 。

T.Yoshida (19??): 有限アーベル群 A と有限群 G に対し、

$$|\mathrm{Hom}(A, G)| \equiv 0 \mod \gcd(|A|, |G|).$$

この定理は、フロベニウスの定理を真似て証明されるので、フロベニウスがこの定理を見つけ、証明していたとしてもおかしくない。したがって、これが新しい定理であるとはきわめて疑わしい。しかし 100 年以上前からの文献をかなり調べても発見できなかった。ホールは知らなかっ

た。1940 年から 1970 年までの有限群論のレビュー (Gorenstein が編集したもの) にも出ていない。そもそもふたつの有限群の間の準同型の個数に関する文献が皆無といってよいほど見あたらない。まったく不思議な話である。

またこの定理が最終型であるとも思えない。実際、上であげたホールのふたつの結果を含まない。証明が間違っている可能性もあると思い、特別の場合に別証明を与えた。まず、A が基本可換 p-群 $C_p{}^r$ の場合は、前節で述べたブラウンのホモロジー論的シローの定理に同値である！ これについては後で述べる。また A が任意のアーベル群で、G が対象群 S_n の場合、指数関数型母関数を考えることによって、また別の証明ができる。一つの問題は上の定理をバーンサイド環の理論を使って証明することである。準同型の個数についてはまだまだやることが残っている。

4. シロー数とフロベニウス数

ここからが本題である。一般に、有限群 G におけるあるタイプの部分群の個数をシロー数と呼び、G 上の方程式の解の個数をフロベニウス数と呼ぼう。以下では、次のようなシロー数とフロベニウス数を考える：

$$\begin{aligned} s(A,G) &:= \sharp\{H \leq G \mid H \cong A\} \\ h(A,G) &:= |\mathrm{Hom}(A,G)|. \end{aligned}$$

A, G は無限群でもかまわない。問題はシロー数とフロベニウス数の関係である。A が巡回群の場合から見て行こう。

C_n を位数 n の巡回群、G を有限群 (または以下の h_n, s_n が任意の n に対し有限であるような群) とし、

$$\begin{aligned} h_n &:= h(C_n,G) = \sharp\{x \in G \mid x^n = 1\} \\ s_n &:= s(C_n,G) = \sharp\{H \leq G \mid H \cong C_n\} \end{aligned}$$

と置く。このとき、次の等式が容易に証明できる。

$$h_n = \sum_{r|n} \varphi(r) s_r, \qquad n \geq 1.$$

ここで$\varphi(r)$ はオイラーの関数 ($\varphi(r)$ は C_r の生成元の個数に等しい)。この等式は、シロー型およびフロベニウス型のゼータ関数を導入すれば、簡潔な形で表現できる：

$$\begin{aligned} S_G^{\mathrm{cyc}}(z) &:= \sum_{n=1}^{\infty} \frac{\varphi(n)\, s_n}{n^z} = \sum_{g \in G} \frac{1}{|g|^z}, \\ H_G^{\mathrm{cyc}}(z) &:= \sum_{n=1}^{\infty} \frac{h_n}{n^z}. \end{aligned}$$

このとき、

$$\boxed{H_G^{\mathrm{cyc}}(z) = \zeta(z)\, S_G^{\mathrm{cyc}}(z)}$$

ここで $\zeta(z)$ はリーマンのゼータ関数である。

また次のように円分恒等式の形にも書ける。

$$\boxed{\prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{\sharp\{g\in G\mid |g|=n\}/n}=\exp\left(\sum_{n=1}^{\infty}\frac{h_n}{n}t^n\right)}$$

以上の議論を巡回群以外の場合に拡張したい。

問題： シロー数とフロベニウス数の関係を見出し、それをなんらかの母関数間の恒等式として表現せよ。

5. Hom-set 行列の LDU-分解と反転公式

有限群 A, B に対し、

$$\begin{aligned}
h(A,B) &:= |\mathrm{Hom}(A,B)| \\
s(A,B) &:= \sharp\{A' \le B \mid A' \cong A\} \\
d(A,B) &:= \begin{cases} |\mathrm{Aut}A| & \text{if } A\cong B \\ 0 & \text{else} \end{cases} \\
q(A,B) &:= \sharp\{A' \trianglelefteq A \mid A/A' \cong B\}
\end{aligned}$$

と置く。これらの数から、有限群の同型類を添字として持つ 4 つの行列 H, S, D, Q を次のように定義する：

$$H := (h(A,B))_{A,B}, \quad S := (s(A,B))_{A,B}$$
$$D := (d(A,B))_{A,B}, \quad Q := (q(A,B))_{A,B}.$$

これらの行列について、理論の鍵となる次の関係がある。

補題 (LDU-分解)： $\boxed{H = QDS}$

同じことだが、有限群 A, G に対し、

$$\boxed{h(A,G)=\sum_{B}{}'\sharp\{A' \trianglelefteq A \mid A/A' \cong B\}\cdot|\mathrm{Aut}A|\, s(B,G)}$$

ここで和は、(A の剰余群に同型な) 有限群の同型類上の和である。

証明は群の準同型定理から容易に得られる。有限群を位数の小さい順に並べると、Q は下 3 角行列になり、S は上 3 角行列になる。さらに D は対角行列である。したがってこの補題は、行列の数値計算でおなじみの LDU-分解を意味する。

簡単な応用として、米田の補題の強化版がある：

$$\begin{aligned}
h(A_1,G) = h(A_2,G)\ \forall G \quad &\Longrightarrow \quad A_1 \cong A_2 \\
h(A,G_1) = h(A,G_2)\ \forall A \quad &\Longrightarrow \quad G_1 \cong G_2
\end{aligned}$$

ここで A_1, A_2, A, G_1, G_2, G は有限群である。

さて上の補題から、$S = D^{-1}Q^{-1}H$ となるが、Q^{-1} の成分をメビウス関数を用いて表わすことができる。

反転公式： $$\boxed{s(A,G) = \frac{1}{|\mathrm{Aut}A|}\sum_{B\trianglelefteq A}\mu_A^{\mathfrak{n}}(1,B)\,h(A/B,G)}$$

ここで $\mu_A^{\mathfrak{n}}$ は、A の正規部分群のなす順序集合のメビウス関数である。

このメビウス関数の値は次の補題を用いて容易に計算できる。

補題： A を有限群、B をその正規部分群とする。このとき

(1) $\mu_A^{\mathfrak{n}}(1,B) \neq 0$ なら，B は、A のいくつかの極小正規部分群の直積（したがって、単純群の直積に同型）である。

(2) $B = Z(B) \times B_1 \times \cdots \times B_r$、ここで B_i は A の極小正規部分群、なら

$$\mu_A^{\mathfrak{n}}(1,B) = (-1)^r\,\mu_A^{\mathfrak{n}}(1,Z(B))$$

(3) B が A のいくつかの可換な極小正規部分群の直積だとする。A の内部自己同型により、B を半単純 A-加群と見なす。$B = B_1 \times \cdots \times B_k$ を等質分解、すなわち各 B_i は A の正規部分群で A-既約成分は互いに同型、さらに $i \neq j$ の時、B_i と B_j の既役成分は A-同型でないとする。このとき

$$\mu_A^{\mathfrak{n}}(1,B) = \prod_{i=1}^{k}\mu_A^{\mathfrak{n}}(1,B_i)$$

(4) p を素数、V を既役 $\mathbf{F}_pA$-加群、$q := |\mathrm{End}(V)|$ とする。A の可換正規部分群 B が、A-加群として rV (V の r個の直和) に同型とする。このとき

$$\mu_A^{\mathfrak{n}}(1,B) = (-1)^n\,q^{\binom{r}{2}}$$

(5) A を p-群、B をその正規部分群とする。このとき

$$\mu_A^{\mathfrak{n}}(1,B) = \begin{cases} (-1)^r p^{\binom{r}{2}} & \text{if } C_p{}^r \cong B \leq \Omega_1(Z(A)) \\ 0 & \text{if } B \not\leq \Omega_1(Z(A)) \end{cases}$$

ここで $\Omega_1(Z(A)) := \langle x \in Z(A) \mid x^p = 1\rangle$ である。

例： 簡単のため、

$$\begin{aligned} h_{ij\cdots} &:= h(C_{p^i} \times C_{p^j} \times \cdots, G) \\ s_{ij\cdots} &:= s(C_{p^i} \times C_{p^j} \times \cdots, G) \end{aligned}$$

と置く。このとき LDU-分解と反転公式は次の形を取る。

$$\begin{aligned} h_1 &= 1 + (p-1)s_1 \\ h_2 &= 1 + (p-1)s_1 + (p^2-p)s_2 \\ h_{11} &= 1 + (p-1)s_1 + (p^2-1)(p^2-p)s_{11} \end{aligned}$$

$$\begin{aligned}(p-1)s_1 &= h_1-1\\ (p^2-p)s_2 &= h_2-h_1\\ (p^2-1)(p^2-p)s_{11} &= h_{11}-(p+1)h_1+p\end{aligned}$$

これらを使うと、次のフロベニウス型合同式

$$h_1\equiv 0 \pmod p,\quad h_2\equiv h_{11}\equiv 0 \pmod{p^2}$$

からシロー型合同式

$$s_1\equiv 1 \pmod p,\quad s_2+s_{11}\equiv 1 \pmod p.$$

が得られる。しかしながら、位数 p^3 以上の群については、同様の議論をしても、フロベニウス型合同式からシロー型合同式は得られない。シロー型合同式は、一般にはフロベニウス型よりもう一段高い p のべきを法とした合同式である。

6. シロー型ゼータ関数(一般論)

前節のフロベニウス数とシロー数との関係を、適当な母関数によって表現したい。$\mathcal{A}$ を有限群の同型類から成る(有限または無限の)クラス、

$$w:\mathcal{A}/\cong \longrightarrow R$$

を重み関数、ここで R は適当な可換位相環である。

シロー型ゼータ関数を次のように定義する。

$$S_w := \sum_{A\in\mathcal{A}}{}' s(A,G)\,w(|A|)$$

ここで $\sum'$ は同型類の完全代表系についての和を意味する。**注:** 以下では主に $\mathcal{A}$ がべき零群から成る場合を考える。この場合、普通は重み関数として $w(A)=f(|A|)/|A|^z$ を取り、R としてディリクレ級数環を取る。指数関数型の母関数については最後に簡単に触れる。

反転公式により、

$$S_w=\sum_{A\in\mathcal{A}}{}'\frac{w(A)}{|\mathrm{Aut}A|}\sum_{C}{}'\sum_{\substack{B\trianglelefteq A\\ A/B\cong C}}\mu_A^{\mathfrak{n}}(1,B)h(C,G)$$

最後の和記号を、群の拡大の言葉で書き換えることができる。特別の場合だけ定理として書いておこう:

定理: 任意の $A\in\mathcal{A}$ がべき零群で、重み関数が位数だけで決まる($w(A)$ を $w(|A|)$ と書く)とすると、

$$\boxed{S_w=\sum_{C,B}{}'\frac{\mu(1,B)w(|B|\cdot|C|)|\mathrm{Ext}(C,B;A)|}{|\mathrm{Aut}\,B|\cdot|\mathrm{Aut}\,C|\cdot|\mathrm{Hom}(C,B)|}h(C,G)}$$

ここで B, C は有限群の同型類の完全代表系上を動き、μ は G の部分群束のメビウス関数である。さらに $\mathrm{Ext}(C, B; \mathcal{A})$ は中心拡大の同値類の集合である：

$$\mathrm{Ext}(C, B; \mathcal{A}) := \{1 \to B \to A(\in \mathcal{A}) \to C \to 1(c.e.)\}/\cong$$

注： 同型類のクラス $\mathcal{A}$ が無限集合の時は、この級数はしばしば収束せず、その場合この定理は意味がない。

例： $\mathcal{A} = \mathcal{C} =$ { 有限巡回群 } で、$w(n) = n^{-z}$ の場合、

$$\begin{aligned} |\mathrm{Aut}(C_n)| &= \varphi(n) \\ |\mathrm{Hom}(C_n, C_m)| &= \gcd(m, n) \\ |\mathrm{Ext}(C, B; \mathcal{A})| &= \varphi(m)\varphi(n) \cdot \gcd(m, n) \end{aligned}$$

したがって

$$\begin{aligned} S_G^{\mathrm{cyc}}(z) &:= \sum_{A \in \mathcal{C}}{}' s(A, G)\,|A|^{-z} \\ &= \sum_{n \geq 1} \frac{s(C_n, G)}{n^z} \\ &= \sum_{m,n} \frac{\mu(m)\, h(C_n, G)}{(mn)^z} \\ &= \zeta(z)^{-1} \sum_{n=1}^{\infty} \frac{h(C_n, G)}{n^z} = \zeta(z)^{-1} H_G^{\mathrm{cyc}}(z) \end{aligned}$$

7. 可換 p-群のクラス $\mathcal{A} = \mathcal{A}_p$

この場合、シロー型およびフロベニウス型のゼータ関数を次で定義する：

$$\begin{aligned} S_G^{\mathrm{Ap}}(x) &:= \sum_{n \geq 0} \sum_{|A| = p^n}{}' s(A, G)\, x^n \\ H_G^{\mathrm{Ap}}(x) &:= \sum_{n=0}^{\infty} \sum_{|A| = p^n}{}' \frac{h(A, G)}{|\mathrm{Aut}\, A|} x^n \end{aligned}$$

ここで $\sum'$ は、位数 p^n のアーベル群の同型類についての和である。このとき次の恒等式が成立する。

定理： 任意の有限群 G と $|x| < p$ に対し、

$$\boxed{\prod_{m=1}^{\infty} (1 - p^{-m} x)^{-1} = \frac{H_G^{\mathrm{Ap}}(x)}{S_G^{\mathrm{Ap}}(x)}}$$

証明： この場合、$B, C \in \mathcal{A}_p$ に対し、

$$\begin{aligned} |\mathrm{Ext}(C,B;\mathcal{A})| &= |\mathrm{Hom}(C,B)| \\ \mu(1,B) &= \begin{cases} (-1)^m p^{\binom{m}{2}} & \text{if } B \cong {C_p}^m \\ 0 & \text{else} \end{cases} \end{aligned}$$

である。重み関数として、$w(p^n) = x^n$ を取ろう。すると前節の定理から、

$$\begin{aligned} S_G^{\mathrm{Ap}}(x) &= \sum_{n\geq 0} \sum_{|A|=p^n}{}' s(A,G)\, x^n = \sum_{A\in\mathcal{A}_p}{}' s(A,G)\, w(|A|) \\ &= \sum_{C,B}{}' \frac{\mu(1,B) w(|B|\cdot|C|)}{|\mathrm{Aut}\, B|\,|\mathrm{Aut}\, C|} h(C,G) \\ &= \sum_{m,n\geq 0} \sum_{|C|=p^n}{}' \frac{(-1)^m p^{\binom{m}{2}} x^{m+n}}{|\mathrm{GL}(m,p)|\cdot|\mathrm{Aut}\, C|} h(C,G) \\ &= \left(\sum_{m=0}^{\infty} \frac{(-1)^m p^{\binom{r}{2}} x^m}{|\mathrm{GL}(m,p)|} \right) \cdot \left(\sum_{n=0}^{\infty} \sum_{|C|=p^n}{}' \frac{h(C,G)}{|\mathrm{Aut}\, C|} x^n \right) \\ &= \prod_{m=1}^{\infty} (1-p^{-m}x) \cdot \left(\sum_{n=0}^{\infty} \sum_{|C|=p^n}{}' \frac{h(C,G)}{|\mathrm{Aut}\, C|} x^n \right). \end{aligned}$$

ここで最後の等式は 2 項定理のいわゆる q-アナログからでる：

$$\sum_{m=0}^{\infty} \frac{(-1)^m p^{\binom{r}{2}} x^m}{|\mathrm{GL}(m,p)|} = \prod_{m=1}^{\infty} (1-p^{-m}x), \qquad |x| < p$$

以上により、

$$S_G^{\mathrm{Ap}}(x) = H_G^{\mathrm{Ap}}(x) \cdot \prod_{m=1}^{\infty} (1-p^{-m}x).$$

系： $\mathcal{A}_p(G)$ を有限群 G の可換 p-部分群の集合とする。このとき、

$$\frac{1}{|\mathcal{A}_p(G)|} \sum_{A}{}' \frac{h(A,G)}{|\mathrm{Aut}\, A|} = \sum_{A}{}' \frac{1}{|\mathrm{Aut}\, A|}$$

ここで和は可換 p-群の同型類上を取る。

実際、

$$\begin{aligned} S_G^{\mathrm{Ap}}(1) &= |\mathcal{A}_p(G)| \\ H_G^{\mathrm{Ap}}(1) &= \sum_{A}{}' \frac{h(A,G)}{|\mathrm{Aut}\, A|} \end{aligned}$$

定理： $$\boxed{\sum_{|A|=p^n}{}' \frac{1}{|\mathrm{Aut}\, A|} = \sum_{\mathrm{rk}(A)=n}{}' \frac{1}{|A|}}$$

(証明) 上の定理で $G=1$ の場合を考えると、$S_G^{\mathrm{Ap}}(x)=1$ で、

$$\begin{aligned} H_1^{\mathrm{Ap}}(x) &= \sum_{n=0}^{\infty} \sum_{|A|=p^n} \frac{x^n}{|\mathrm{Aut}\, A|} \\ &= \prod_{m=1}^{\infty} (1-p^{-m}x)^{-1} \end{aligned}$$

次の公式は良く知られている：

$$\begin{aligned} \prod_{m=1}^{\infty} (1-p^{-m}x)^{-1} &= \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} p(k,n)\, p^{-k} x^n \\ &= \sum_{A}{}' \frac{1}{|A|}\, x^{\mathrm{rk}(A)} \end{aligned}$$

ここで $p(k,n)$ は、自然数 k を n 個の部分に分割する方法 (すなわち位数 p^k で n 個の生成元を持つ可換 p-群の同型類) の個数：

$$p(k,n) := \sharp\{A \in \mathcal{A}_p/\cong \mid \mathrm{rk}(A)=n, |A|=p^k\}$$

したがって、

$$\boxed{\sum_{n=0}^{\infty} \sum_{|A|=p^n}{}' \frac{x^n}{|\mathrm{Aut}\, A|} = \sum_{A}{}' \frac{1}{|A|}\, x^{\mathrm{rk}(A)}}$$

x^n の係数を比較すれば、定理が得られる。 (証明終)

例： $n=2$ の場合、

$$\begin{aligned} \mathrm{LHS} &= \frac{1}{p^2-p} + \frac{1}{(p^2-1)(p^2-p)} \\ \mathrm{RHS} &= \sum_{1\le i\le j} \frac{1}{p^{i+j}} = \frac{p}{(p-1)(p^2-1)} \end{aligned}$$

上の定理で n についての和を取ると P.Hall による次の奇妙な公式が得られる。

P.Hall (1938): $\boxed{\displaystyle\sum_{A}{}' \frac{1}{|\mathrm{Aut}\, A|} = \sum_{A}{}' \frac{1}{|A|}}$

ここで和は可換 p-群の同型類をについてのものである。

ところで、ここで与えたホールの等式の証明では、左辺の評価では有限アーベル群の分類を使わなかった (と思う)。一方、ホール自身の証明では分類を使い自然数の分割についての和として左辺を計算している。巡回群の直積であるような 可換 p-群を "known" と呼ぶことにすると、ふたつの証明は、実は

$$\sum_{\text{known}}{}' \frac{1}{|\mathrm{Aut}\, A|} \overset{\mathrm{H}}{=} \sum_{\text{known}}{}' \frac{1}{|A|} \overset{\mathrm{Y}}{=} \sum_{\text{all}}{}' \frac{1}{|\mathrm{Aut}\, A|}$$

ということを意味する。したがってすべての可換 p-群は known である。

8. 基本可換 p-群のクラス $\mathcal{A}=\mathcal{E}_p$

この場合、$|\mathrm{Ext}(C_p{}^s, C_p{}^r; \mathcal{A})| = 1$ である。次のような記号を導入する：

$$\begin{aligned}
\begin{bmatrix} n \\ r \end{bmatrix} &:= \sharp\{B \subseteq C_p{}^n \mid |B| = p^r\} = \frac{[p]_n}{[p]_r \cdot [p]_{n-r}} \\
[p]_n &:= (p-1)(p^2-1)\cdots(p^n-1) \\
|\mathrm{GL}(r,p)| &= p^{\binom{r}{2}}[p]_r, \quad \mu(1, C_p{}^r) = (-1)^r p^{\binom{r}{2}}
\end{aligned}$$

この記号を用いると、LDU-分解と反転公式は次のようになる：

$$\begin{aligned}
h(C_p{}^n, G) &= \sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix} |\mathrm{GL}(r,p)|\, s(C_p{}^r, G) \\
s(C_p{}^n, G) &= \frac{1}{|\mathrm{GL}(n,p)|} \sum_{r=0}^{n} (-1)^r p^{\binom{r}{2}} \begin{bmatrix} n \\ r \end{bmatrix} h(C_p{}^{n-r}, G)
\end{aligned}$$

重み関数として $w(p^n) = f(n)x^n$ を取ると、シロー型ゼータ関数について、

$$\begin{aligned}
S_G^{\mathrm{Ep}}(x) &:= \sum_{n\geq 0} s(C_p{}^n, G) f(n) x^n \\
&= \sum_{r,s\geq 0} \frac{(-1)^r f(r+s) h(C_p{}^s, G)}{|\mathrm{GL}(r,p)| \cdot |\mathrm{GL}(s,p)| \cdot p^{rs}} p^{\binom{r}{2}} x^{r+s} \\
&= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{f(r+n)}{[p]_r} (-p^{-n}x)^r \right) \frac{h(C_p{}^n, G)}{|\mathrm{GL}(n,p)|} x^n
\end{aligned}$$

が成り立つ。

(1) $f(p^n) = 1$ の場合：この場合、$|x| < p$ に対し、

$$\begin{aligned}
S_G^{\mathrm{Ep}}(x) &:= \sum_{n\geq 0} s(C_p{}^n, G) x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{1}{[p]_r} (-p^{-n}x)^r \right) \frac{h(C_p{}^n, G)}{|\mathrm{GL}(n,p)|} x^n \\
&= \left(\prod_{r=1}^{\infty} (1 - p^{-r}x) \right) \cdot \sum_{n=0}^{\infty} \left(\prod_{r=1}^{n} (1-p^{-r}x)^{-1} \right) \frac{h(C_p{}^n, G)}{|\mathrm{GL}(n,p)|} x^n
\end{aligned}$$

となる。特に、$G = 1$ とすると、$S_G^{\mathrm{Ep}}(x) = 1$ かつ $h(C_p{}^n, G) = 1$ である。したがって上の等式より、コーシー (1893) による次の公式が得られる ([An 76] Cor. 2.6)：

$$\boxed{\prod_{r=1}^{\infty} (1-p^{-r}x)^{-1} = \sum_{n=0}^{\infty} \frac{x^n}{|\mathrm{GL}(n,p)| \cdot \prod_{i=1}^{n} (1-p^{-i}x)}}$$

$x \to 1$ として、次の公式 (オイラー) を得る：

$$\boxed{\prod_{r=1}^{\infty}(1-p^{-r})^{-1}=\sum_{n=0}^{\infty}\frac{p^n}{\prod_{i=1}^{n}(p^i-1)^2}}$$

$(2) f(p^n)=p^{\binom{n}{2}}$ の場合：この場合、$|x|<p$ に対し、

$$\begin{aligned} S_{G,f}^{Ep}(x) &:= \sum_{n\geq 0} s({C_p}^n,G)p^{\binom{n}{2}}x^n \\ &= \prod_{n=1}^{\infty}(1+p^{-n}x)^{-1}\cdot\sum_{n=0}^{\infty}\frac{h({C_p}^n,G)}{[p]_n}x^n \end{aligned}$$

このゼータ関数について、

補題： $\boxed{S_{G,f}^{Ep}(-1)=1-\chi(\mathcal{S}_p)}$

ここで前と同様に、$\chi(\mathcal{S}_p)$ は、G の自明でない p-部分群のなす順序集合のオイラー標数である。

これを使うと、

$$h({C_p}^n,G)\equiv 1-\chi(\mathcal{S}_p) \mod \gcd(p^n,|G|)$$

が得られる。すなわち、3 節で述べたフロベニウスの定理の拡張とブラウンのホモロジー論的シローの定理は同値である。

9. p-群 の ク ラ ス $\mathcal{A}=\mathcal{G}_p$

この場合、

$$\begin{aligned} |\mathrm{Ext}(P,{C_p}^r;\mathcal{G}_p)| &= |\mathrm{H}^2(P,\mathbb{Z}/p\mathbb{Z})|^r \\ |\mathrm{Hom}(P,{C_p}^r)| &= |\mathrm{H}^1(P,\mathbb{Z}/p\mathbb{Z})|^r=|P/\Phi(P)|^r \\ \mu(1,B) &= \begin{cases} (-1)^r p^{\binom{r}{2}} & \text{if } B\cong {C_p}^r \\ 0 & \text{else} \end{cases} \end{aligned}$$

となる。さらに、

$$\eta(P):=\frac{|\mathrm{H}^2(P,\mathbb{Z}/p\mathbb{Z})|}{|\mathrm{H}^1(P,\mathbb{Z}/p\mathbb{Z})|}$$

と置く。N を十分大きな整数 ($p^N\geq |G|_p$ なら良い) とする。このとき、

$$\begin{aligned} S_G^{\mathrm{Gp}}(x) &:= \sum_{n\geq 0}\sum_{|P|=p^n}{}' s(P,G)\,x^n \\ &= \sum_{C,B}{}'\frac{\mu(1,B)w(|B|\cdot|C|)|\mathrm{Ext}(C,B;\mathcal{G}_p)|}{|\mathrm{Aut}\,B|\cdot|\mathrm{Aut}\,C|\cdot|\mathrm{Hom}(C,B)|}h(C,G) \\ &= \sum_{n=0}^{N}\sum_{|P|=p^n}{}'\left(\sum_{r=0}^{N-n}\frac{(-1)^r p^{\binom{r}{2}}\eta(P)^r x^r}{|\mathrm{GL}(r,p)|}\right)\frac{h(P,G)}{|\mathrm{Aut}\,P|}x^n \\ &= \sum_{n=0}^{N}\sum_{|P|=p^n}{}'\left(\sum_{r=0}^{N-n}\frac{(-\eta(P))^r}{[p]_r}x^r\right)\frac{h(P,G)}{|\mathrm{Aut}\,P|}x^n \end{aligned}$$

となる。ここで2番目の和で、C は位数高々 p^N の群を動く。まずいことに、最後の級数は $N \to \infty$ のもとで、発散する。実際、P が位数 p^n で極小生成元の個数が d のとき、

$$\binom{d}{2} \leq \log_p \eta(P) \leq \binom{n}{2}$$

が成立し、したがって $\lim_{d\to\infty} \eta(P) = \infty$ となるからである (Golod–Safarevic, Wiegold, Jones)。このことは昔、類体塔の非存在の証明で使われた。

10. 書き残した事柄

(1) 前節のように、シロー型ゼータ関数をフロベニウス型ゼータ関数で表示しようとするとき、しばしば収束しない級数に出会う。それを避けるには、うまい重み関数を見つけることの他にも、べき級数を p-進べき級数と考える方法がある。

(2) いろいろな恒等式を、ここで述べてきたような「群論的方法」で証明することは、興味ある問題である。例えば、オイラーの5角数定理

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{m=-\infty}^{\infty}(-1)^m x^{m(3m-1)/2}$$

をここで述べたような方法で証明できないものだろうか。

(3) これまで述べてきたシロー数 $s(A,G)$ やフロベニウス数 $h(A,G)$ の考察では、G を固定し、A を動かしたときの母関数を考えた。これと反対に、A を固定し、G を動かしたときの母関数も考えられる。G として対称群を取った場合が既に研究の対象になっている。

A を有限生成の群、S_n を n 次対称群とし、

$$h_n(A) := h(A, S_n) = |\mathrm{Hom}(A, S_n)|$$

と置く。このとき、

$$\sum_{n=0}^{\infty}\frac{h_n(A)}{n!}t^n = \exp\left(\sum_{B\leq A}\frac{1}{(A:B)}t^{(A:B)}\right)$$

ここで B は A の指数有限の部分群全体をわたる。これは、K.Wohlfahrt [Wo 77] の公式である。他にも何人かの人が独立にこの公式を発見している。これに同値な $h_n(A)$ に関する漸化式は、I.Dey [De 65] にある。彼らはこれらの公式を、自由群やモジュラー群の与えられた指数の部分群の個数を求めるというシロー型の問題に使った。また制限バーンサイド問題への応用がある.

(4) $A = \hat{\mathbb{Z}}_p$ を p-進整数環の加法群とする。このときフロベニウスの定理より、

$$h_n(\hat{\mathbb{Z}}_p) = \sharp\{p\text{-element of } S_n\} \equiv 0 \bmod (n!)_p,$$

である。すなわち $h_n(\hat{\mathbb{Z}}_p)/n! \in \hat{\mathbb{Z}}_p$。これはアルチン・ハッセの指数関数

$$E_p(t) := \exp\left(\sum_{r=0}^{\infty}p^{-r}t^{p^r}\right) = \sum_{n=0}^{\infty}\frac{h_n(\hat{\mathbb{Z}}_p)}{n!}t^n$$

が、$\nu_p(t) > 0$ (ただし、$\nu_p(p^e) = e$) で (p-進べき級数として) 収束することを意味する ([Ko 77] IV.2)。

(5) $h_n(A)$ が素数 p の何乗で割り切れるかという問題は、$p = 3, A = C_3$ の場合でさえ難しい。

(6) シロー型ゼータ関数とフロベニウス型ゼータ関数を結ぶ公式において、G が自明な群の場合でさえ、自明でない結果 (例えばホールの奇妙な公式やコーシーの恒等式) が得られた。これも奇妙な話であるが、自明でない結果が得られた理由は、Hom-set 行列の LDU-分解にある。ここで述べてきたいろいろな公式の背景には、巡回群、可換群、可換 p-群、基本可換 p-群、p-群といった種類の群のカテゴリーでは、射が全射と単射の合成として一意的分解する、ということがある。本当は、初めに、そのような性質を持つカテゴリーの「抽象バーンサイド環」なるものの理論があり、それを有限群のカテゴリーに使ってみたら、これまで述べてきた定理や公式や別証明などが出てきたのである ([Yo 87] 参照)。

References

[An 76] G.E.ANDREWS, "The Theory of Partitions ", in *Encyclopedia of Mathematics and its Applications* vol. 2, 1976.

[Br 75] K.BROWN, Euler characteristics of groups : The p-fractional part, *Invent. Math.* **29** (1975), 414–430.

[BT 88] K.BROWN–J.THÉVENAZ, A generalization of Sylow's third theorem, *J. Algebra* **115** (1988), 414–430.

[Di 79] T. TOM DIECK, "Transformation Groups and Representation Theory ", *LNS in Math.* **766**, Springer, 1979.

[DSY ??] A.DRESS–C.SIEBENEICHER–T.YOSHIDA, An application of Burside rings in elementary finite group theory, *Adv. Math.* (to appear).

[Gl 81] D.GLUCK, Idempotent formulae for the Burnside algebtra with applications to the p–subgroup simplicial complexes, *Illinois J.Math.*, **25** (1981).

[Ha 35] P.HALL, On Frobenius theorem, *Proc. London Math. Soc.*(2) **40** (1935), 468–501.

[Ha 38] P.HALL, A partition formula connected with abelian groups, *Comment, Math. Helv,* **11** (1938), 126–129.

[It 89] 伊藤昇「Ludvig Sylow 伝」 Basic 数学、1989 年 9 月号, 44–49.

[Ko 78] N.KOBLITZ, "p-adic Numbers, p-adic Analysis, and Zeta–Functions", Springer, 1977.

[Qu 78] D.QUILLEN, Homotopy propoerties of the poset of non-trivial p-subgroups of a group, *Adv. Math.* **28** (1978), 101–128.

[So 62] L.SOLOMON, The Schur's index and the solutions of $G^n = 1$ in a finite group, *Math.Z.*, **70** (1962), 122–125.

[So 62] L.SOLOMON, The solution of equations in groups, *Arch.Math.*, **20** (1969), 241–247.

[Wa 80] B.WAGNER, A permutation representation theoretical version of a theorem of Frobenius, *Bayreuther Math.* **6** (1980), 23–32.

[Wo 77] K.WOHNFAHRT, Über einen Satz von Dey und die Modulgruppe, *Arch, Math.* **29** (1977)

[Yo 83] T.YOSHIDA, Idempotents of Burnside rings and Dress induction thoerem, *J. Algebra* **80** (1983), 90–105.

[Yo 87] T.YOSHIDA, On the Burnside rings of finite groups and finite categories, *Advanced Studies in Pure Mathematics* **11** (1987), 337–353.

[Yo ??] T.YOSHIDA, $|\mathrm{Hom}(A,G)|$, *J.Algebra*, in printing.